AN EMBEDDED CRYPTOSYSTEM IMPLEMENTING SYMMETRIC CIPHER AND PUBLIC-KEY CRYPTO ALGORITHMS IN HARDWARE

HAU YUAN WEN

UNIVERSITI TEKNOLOGI MALAYSIA

AN EMBEDDED CRYPTOSYSTEM IMPLEMENTING SYMMETRIC CIPHER AND PUBLIC-KEY CRYPTO ALGORITHMS IN HARDWARE

HAU YUAN WEN

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Engineering (Electrical)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

SEPTEMBER 2005

Specially dedicated to
my dearest family and beloved Kheng Boon

ACKNOWLEDGEMENTS

The first person I would like to express my gratitude is my supervisor, Professor Dr. Haji Mohamed Khalil bin Haji Mohd Hani for his invaluable support, patience and unbounded enthusiasm throughout this work. Thanks for helping me to kickstart this research by providing insights and his working experience as reference. His overly enthusiasm and integral view on research and his mission for providing only high-quality work and not less, has made a deep impression on me. I am truly grateful for having such a wonderful supervisor.

I would also like to convey my gratitude to my lecturers, Encik Nadzir Marsono, Encik Nasir Shaikh Husin, and to my seniors Kie Woon, Avinash, Yew Leong, Eng Kean and J-Wing for tirelessly guiding me through my research journey. I would also like to thank to my friends, Arul, Kwee Siong, Eng Yew and Leong Shian. I value the camaraderie we share as well as the time they spent to share with me enriching ideas, as well as their concern. I truly admire them for their capability and kindness to offer help whenver they can. Many thanks also to our hardworking technicians in ECAD lab, En. Zulkffli bin Che Embong and En. Khomarudden bin Mohd Khair Juhari.

My sincerest thanks to all those who have helped to make this thesis possible. Warmest regards to my parents and siblings for their seamless caring encouragement and moral support that enable this journey. Without exception, a special thanks to Kheng Boon for his consistent encouragement and concern over time. Without his unwavering support, love and devotion through the years, this thesis could not have been realized.

ABSTRACT

Information security in terms of confidentiality, data integrity, non-repudiation and authentication is one of the critical aspects in majority of electronic communication and computer networks, especially in high speed security system. This thesis proposes an embedded cryptosystem design prototype, which consist of hybrid encryption cryptosystem and ECC-based digital signature cryptosystem, to provide all of the mentioned security services. The cryptosystem is designed using hardware-software codesign technique. The cryptosystem composes of three components: (a) hardware processing module, (b) device driver and (c) Application Programming Interface (API). This project focused on the bus interface module design of several in-house designed processor cores, which include ECC, RSA, SHA-1 and AES crypto processor core, and LZSS data compression processor core. Besides, a supplementary large integer Modular Arithmetic processor core (MAP), is designed as part of this work. All of these processor cores have been integrated to form a complete cryptosystem in SoPC environment together with Nios main processor and standard peripherals. The embedded device drivers and APIs have been scripted to communicate with each dedicated coprocessor and cryptosystem. The embedded cryptosystem is implemented on an Altera Stratix FPGA prototyping board with an operating system frequency at 40 MHz. An application demonstration prototype and real-time e-document security application has been developed to test the functionality and robustness of the cryptosystem as well as the usability of the embedded device drivers and the APIs. The hybrid encryption cryptosystem offers a performance of 1.80 Mbps in AES crypto subsystem, and able to execute RSA full modular exponentiation operation in just 53 ms. Besides, the ECC-based digital signature cryptosystem can compute the ECDSA signing and verification in a finite field of $GF(2^{163})$ in 0.59 ms and 1.06 ms, respectively. As the result, this embedded cryptosystem is suitable for next generation real-time IT security.

ABSTRAK

Keselamatan maklumat merupakan aspek yang paling kritikal di dalam kebanyakan rangkaian komunikasi eletronik dan computer, terutamanya di dalam sistem kelajuan tinggi. Ini meliputi aspek kesulitan maklumat, kewibawaan data, kesahihan serta pengesahan. Tesis ini mencadangkan satu prototaip sistem kripto terbenam yang terdiri daripada sistem kripto enkripsi hybrid dan sistem kripto tandatangan digital berbasis ECC, untuk membekalkan semua perkhidmatan keselamatan tersebut. Sistem kripto ini direkacipta dengan menggunakan teknik co-rekacipta perkakasan-perisian. Ia terdiri daripada tiga komponen: (a) modul pemproses perkakasan, (b) pemacu peranti dan (c) antara muka pengaturcaraan aplikasi (*API)*. Projek ini fokus kepada rekacipta modul bus perantaraan muka kepada beberapa teras pemproses rekacipta dalaman, termasuk ECC, RSA, SHA-1 and AES teras pemproses kripto, dan teras pemproses LZSS pemampatan maklumat. Selain itu, sebuah teras pemproses aritmetik modular (*MAP*) tambahan juga direkacipta. Kesemua teras pemproses ini telah digabungkan untuk membentuk sebuah sistem kripto yang lengkap menerusi SoPC bersama dengan pemproses utama Nios serta persisian langsung. Pemacu peranti terbenam dan *API* telah diskripkan untuk berkomunikasi dengan co-pemproses dan sistem kripto. Sistem kripto terbenam tersebut telah diimplementasikan pada sebuah papan prototaip Stratix FPGA Altera pada frekuensi 40 MHz. Sebuah prototaip aplikasi demonstrasi dan aplikasi keselamatan e-dokumen masa-nyata telah dibangunkan untuk menguji fungsi serta ketegapan sistem kripto bersama-sama dengan penggunaan pemacu peranti terbenam dan *API*. Sistem kripto enkripsi hybrid ini menawarkan prestasi 1.80 Mbps dalam subsistem kripto AES, dan mampu melaksanakan operasi exponensasi bermodul penuh RSA dalam tempoh hanya 53 ms. Di samping itu, sistem kripto tandatangan digital berbasis ECC ini boleh mengira tandatangan dan pengesahan ECDSA pada medan terhinggan $GF(2^{163})$ dalam 0.59 ms dan 1.06 ms masing-masing. Kesimpulannya, sistem kripto terbenam ini adalah sesuai untuk keselamatan informasi teknologi masa-nyata pada generasi yang seterusnya.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

.bdf	-	Block Diagram File
AES	-	Advanced Encryption Standard
API	-	Application Programming Interface
ASIC	-	Application Sppecific Integrated Circuit
CA	-	Certificate Authority
CAD	-	Computer Aided Design
CPU	-	Centre Processing Unit
DES	-	Data Encryption Standard
DLP	-	Discrete Logatirhm Problem
DMA	-	Direct Memory Access
DSA	-	Digital Signature Standard
DSP	-	Digital Signal Processing
DVD	-	Digital Video Disc
ECC	-	Elliptic Curve Cryptography
ECDH	-	Elliptic Curve Diffie Hellman
ECDLP	-	Elliptic Curve Discrete Logarithm Problem
ECES	-	Elliptic Curve Encryption Standard
ECDSA	-	Elliptic Curve Digital Signature Algorithm
ECP	-	Elliptic Curve Processor
EDA	-	Electronic Design Automation
F_{max}	-	Maximum Frequency
FPGA	-	Field Programmable Gate Array
FIPS	-	Federal Information Processing Standard
FTP	-	File Transfer Protocol
GF	-	Galois Field
GUI	-	Graphical User Interface

HSM	-	Hardware Security Module
IC	-	Integrated Circuit
IFP	-	Integer Factorization Problem
I/O	-	Input/Output
IP	-	Intellectual Property
IT	-	Information Technology
LAN	-	Local Area Network
LE	-	Logic Element
LSB	-	Least Significant Bit
LZSS	-	Lempel-Ziv-Storer-Szymanski
MAC	-	Message Authentication Code
MAP	-	Modular Arithmetic Processor
MHz	-	Mega Heartz
MSB	-	Most Significant Bit
PC	-	Personal Computer
PCI	-	Peripheral Component Interconnect
PIO	-	Parallel Input Output
PKI	-	Public Key Infrastructure
PLD	-	Programmable Logic Device
PRNG	-	Pseudo Random Number Generator
RAM	-	Random Access Memory
RISC	-	Reduced Instruction Set Computer
RTDS	-	Real Time Data Security
ROM	-	Read Only Memory
RSA	-	Rivest-Shamir-Adleman
SDK	-	System Development Kit
SHA-1	-	Secure Hash Algorithm
SoC	-	System-on-Chip
SOPC	-	System-on-Programmable-Chip
SPI	-	Serial Peripheral Interface
SRAM	-	Static RAM
UART	-	Universal Asymchronous Receiver Transmitter
USB	-	Universal Serial Bus
VCR	-	Video Casette Recorder

VHDL - Very High Speed Integrated Circuit Hardware Description Language

WAP - Wireless Application Protocol

VB - Visual Basic

VLSI - Very Large Scale Integration

LIST OF APPENDICES

PART ONE
THESIS CONTENT

CHAPTER 1

INTRODUCTION

This thesis proposes the FPGA implementation of an embedded cryptosystem. The design applies the System-on-Chip (SoC) technology to produce a hardware security module that performs operation such as encryption, decryption, digital signature signing and verification, etc. This chapter covers the background, problem statement, research objectives, scope of work, the significance and contribution of the research, and finally thesis organization.

1.1 Background

Nowadays, it is difficult to open a newspaper, watch a television program, or even have a conversation without some mention of the Internet, e-commerce, WAP and m-commerce. The rapid progress in wireless communication system, personal communication system, and smart card technology in our society makes information more vulnerable to abuse. In a communication system, the content of the communication may be exposed to an eavesdropper, or system services can be used fraudulently. For these reasons, it is important to make information systems secure by protecting data and resources from malicious acts.

Today, embedded systems have become increasingly popular, as advances in IC-technology and processor architectures allow for flexible computational parts and high-performance modules integrated on a single carrier. An embedded system may

be defined as hardware system incorporating general-purpose computational units and several dedicated modules. Typical embedded system include digital camera, digital camcorder, VCR, DVD, etc. They perform a specific function carefully partitioned in software and hardware to strike the balance between flexibility, reusability, performance and cost.

In today's state-of-the-art technology, many of the embedded system or substantial parts of the systems can be integrated on a single microchip. System-on-a-chip (SoC) technology is a programmable platform that integrates most of the functions of an end product into a single chip. It incorporates at least one processing element (e.g. microprocessor, DSP) that executes the embedded software. The system is completed with peripherals random logic and interfaces to the outside world and employs a bus-based architecture. Figure 1.1 shows an example of SoC-based embedded system. Design reuse and intellectual property (IP) sharing for both hardware and software are critical for high productivity in designing SoC. Therefore, SoC requires core-based design techniques, which utilize available hardware and software cores and compose them by adding appropriate interface to generate new designs (Li, 1998).

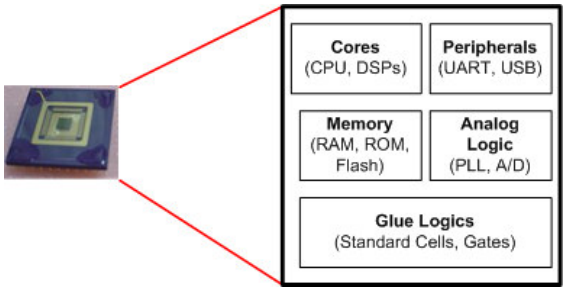

Figure 1.1 SoC Integration

1.2 Problem Statement

As mentioned earlier in previous section, it is important to make information systems secure by protecting data and resources from malicious acts or being abused.

IT security can be provided by crypto (cryptographic) solutions. Cryptography is, in general, the science of concealing data. It uses mathematical algorithms and processes to convert intelligible plaintext into unintelligible ciphertext, and vice versa. A crypto solution can provide four security services, which is **authentication**, **non-repudiation**, **data integrity** and **confidentiality**. The first three services are typically provided by digital signature and confidentiality is typically provided by encryption (Certicom, 1998).

The two main types of cryptography are symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography schemes require two parties who want to communicate in confidence to share a common, secret key. Each user must trust the other not to divulge the common key to a third party. These systems encrypt large amounts of data efficiently. However, they pose significant key management problems in networks of large number of users. Public key cryptography schemes require each part to have a key pair: a private key, which must not be disclosed to another user, and a public key, which may be made available in a public directory. The two keys are related by a one–way function, so it is computationally infeasible to determine the private key from the public key. Public key systems solve the key management problems associated with symmetric key encryption. Even more importantly, public key cryptography offers the ability to efficiently implement digital signatures (RSA, 1999). However, its speed is slow in encryption of large amount of data compared with symmetric key cryptography. The complete solution is to combine both of the symmetric key cryptography and public key cryptography to compliment each other into a well-defined framework, such as Public Key Infrastructure (PKI) (Sun, 2001).

Crypto algorithm can be implemented in either hardware or software. It is fairly easy to implement crypto algorithms in software, but such approach is typically too slow for real-time applications such as storage devices, embedded system, etc. Hence, for these kinds of applications, hardware always appears to be the ultimate choice of implementation. As coprocessors, they can offload time-consuming algorithms and reduce the computation bottleneck (Lejla *et al*., 2003). For any same operation and function, hardware implementation will always outperform software

implementation in timing performance. Crypto hardware accelerators are not only faster in general, but also offer at the same time more intrinsic security. Unlike software implementations, crypto hardware is resistant to physical tampering. This is one of the most important features of the crypto hardware. In addition, crypto hardware also cannot be cloned easily, hacked, modify, etc. Therefore, it is suitable to be used in many of the critical real-time applications.

In the hardware implementation, the FPGA (Field Programmable Gate Array) has become the chosen rapid prototyping platform for any proof-of-concept design, before being committed to an ASIC (Application-Specific Integrated Circuit) or VLSI implementation. The flexibility and reconfigurability of FPGAs make them suitable platform for implementations of crypto hardware embedded systems.

1.3 Objectives

From the discussion above, this thesis sets out two objectives:

1. To design an embedded cryptosystem that integrates several dedicated IP cores. The IP cores include four crypto coprocessors, which perform elliptic curve cryptography (ECC), SHA-1 hashing, AES Encryption and RSA public-key crypto algorithm. These processors are complemented with LZSS (Lempel-Ziv-Storer-Szymanski) data compression core and large integer Modular Arithmetic Processor (MAP) core and a 32-bit CPU. The embedded system is designed using SoC technology in a single FPGA chip.

2. To develop a hardware security module, that incorporates the cryptosystem in (1) to perform the security functions of data confidentiality, data integrity, non-repudiation and authentication. To achieve these functions, the security mechanisms will include symmetric encryption, digital signature, and public-key cryptography. A secure e-document application is developed as a demonstration application prototype to validate the proposed cryptosystem in a real-world case.

1.4 Scope of Work

1. The embedded cryptosystem is designed in VHDL. It implements a 128-bit AES algorithm for message encryption, 1024-bit RSA for public-key encryption, and 163-bit elliptic curve (ECC) public-key cryptography for digital signature.

2. The system provides a suitable compromise between the constraints of speed, space and required security level based on the specific demands of targeted application. This is achieved with parameterization in the design.

3. The complete prototype is to fit into an Altera Stratix EP1S40F780C5 FPGA chip (which contains 41250 LEs (Logic Elements) or an equivalent of 14 x 10^6 system gates). The current cryptosystem's running frequency is limited to 40 MHz. Figure 1.2 shows the system architecture showing the host and proposed embedded cryptosystem.

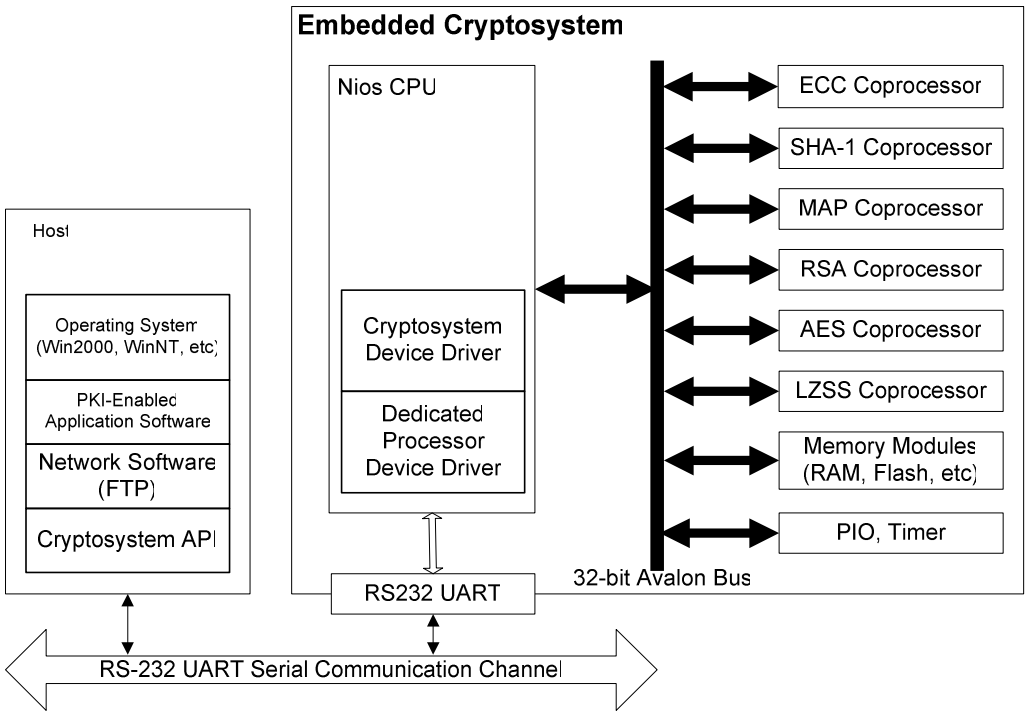

Figure 1.2 System Architecture

4. With VHDL parameterization, the RSA and ECC coprocessor can be reconfigured to other key sizes, based on the security level and the hardware resources required by targeted application.

5. The current version of the proposed cryptosystem does not include on-chip, the ECC system parameter generation and RSA key pair generation. The current version is able to sign / verify and encrypt /decrypt a file limited to size of not more than 512 MB and 4 GB, respectively. For a file larger than these sizes, the file needs to be chopped into multiple smaller files.

6. The cryptosystem is validated by a secure e-document application through a Local Area Network (LAN).

1.5 Research Contribution and Project Delivery

1. An advanced security processor hardware for next-generation IT security is proposed. It incorporates a 32-bit RISC embedded general-purpose Nios processor together with six IP modules including ECC, RSA, SHA, AES, LZSS and MAP.

2. Introduce and establish a systematic design approach to design an embedded system in a SoC environment based around the Altera NIOS™ embedded processor using hardware/software codesign techniques.

3. Deliver an application demonstration prototype in the form of an examination security application, which demonstrates the transfer of confidential document through insecure electronic network.

1.6 Thesis Organization

The thesis is organized into eight chapters. The first chapter introduces the motivation, research objectives, research scope, research contribution and together with thesis organization.

Chapter 2 reviews the background of the research. Related works similar to this field are presented. Summary of the literature review is given to clarify the research rationale.

Chapter 3 describes the research methodology, system design procedures and application tools that have been used in this research.

Chapter 4 presents the design of a hybrid cipher cryptosystem for message encryption, while Chapter 5 presents the design of ECC-based public key digital signature cryptosystem. These two chapters discuss in terms of hardware block design, device driver and API development.

Chapter 6 reports the hardware test and performance studies on the proposed hybrid encryption cryptosystem and public key digital signature cryptosystem and their related coprocessor. Comparison between the proposed embedded cryptosystem and previous implementations is made.

Chapter 7 describes the software development of application demonstration prototype, which is a real-time e-document transmission via insecure channel. This application demonstration prototype is used to test the functionality of the embedded cryptosystem, as well as embedded device drivers and APIs.

In the final chapter, the research work is summarized and the potential future works are given.

the parameters in a reconfigurable cryptosystem only takes place after certain period of time. Besides, the device driver can be improved to include the other ECC-based cryptography algorithms such as Elliptic Curve Diffie Hellman (ECDH) scheme, Elliptic Curve Encryption Standard (ECES) scheme, etc. As such, the cryptosystem is general to all ECC-based cryptography algorithm schemes instead of just limited to digital signature.

The same recommendation is applied to RSA cryptosystem device driver. Instead of just encrypt the symmetric session key, the RSA device driver can be improved to implement the RSA public key encryption and digital signature since their underlying mathematic operation is same, which is modular exponentiation operation. Besides, the device driver should include a most important operation, which is on-chip RSA public key and private key generation together with the required Montgomery parameters to meet the requirement of the RSA coprocessor.

Besides, it is recommended that the future work implements digital certificate scheme which is compliant to X.509 format for e-commerce application. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority (CA).

The next recommendation of the future work is the improvement of API. The API of the SHA160 coprocessor can be improved to enable message digest computation of file size less than 2^{64} bits instead of just 2^{32} bits (512 MB) to meet the FIPS standard. Besides, the API of the AES subsystem can be improved to encrypt a file with arbitrary length instead of limited to 4 GB.

To enhance the data security level, the random number generation needed in symmetric key encryption and digital signature signing and key pair generation should be truly random generated instead of pseudo random generated. This can be achieved by design a true random number generator in hardware by capturing the signal noise or system timer.

The MAP163 arithmetic coprocessor with maximum frequency of 41.62 MHz becomes the bottleneck of the entire cryptosystem. Therefore, the design architecture of the MAP163 can be improved based on some advanced algorithm such as Montgomery algorithm or more sophisticated architecture such as systolic array implementation. This will improve the maximum frequency of the coprocessor and improve the maximum system frequency of the embedded cryptosystem directly.

From the discussion on the previous chapter, it can be concluded that the ECC proves to be a viable alternative to the RSA and may become the potential replacement of RSA cryptography in security devices for future generations. However, for the purpose of hardware compatibility and interoperability for future security devices, a common hardware platform for both RSA and ECC cryptography needs to be designed to reduce the hardware resources.

In this work, the interfacing between API and device driver to control the hardware processing blocks to perform core operation is through UART serial communication port. This has contributes to the high software overhead of the file manipulation. The interface can be upgraded to Universal Serial Bus (USB) communication to reduce the software overhead. Besides, in the embedded cryptosystem, the Nios DMA (Direct Memory Access) module in the Altera SOPC Builder library can be included to allow efficient bulk data transfer between peripherals and memory. It can be used to perform DMA data transfer between two memories, between a memory and a peripheral, or between two peripherals without intervention from the Nios main embedded processor.

REFERENCES

Altera Corporation. (2003a). *Nios 3.0 CPU Data Sheet*. Altera Corporation.

Altera Corporation. (2003b). *Nios Embedded Processor: Software Development Reference Manual*. Altera Corporation.

Altera Corporation. (2003c). *Nios Hardware Development Tutorial*. Altera Corporation.

Altera Corporation. (2003d). *Introduction to Quartus II*. Altera Corporation.

Altera Corporation (2003e). *Nios Development Board: Reference Manual, Stratix Professional Edition*. Altera Corporation.

Altera Corporation. (2003f). *SOPC Builder Data Sheet*. Altera Corporation.

Altera Corporation. (2003g). *Avalon Bus Specification: Reference Manual*. Altera Corporation.

Altera Corporation. (2003h). *Stratix Device Handbook: Volume 1*. Altera Corporation.

Altera Corporation. (2003i). *Nios Timer Data Sheet*. Altera Corporation.

Aydos M. (2001). *Efficient Wireless Security Protocols based on Elliptic Curve Cryptography*. Oregon State University: Ph.D. Dissertation.

Brown M., Hankerson D., Lopez J., and Menezes A. (2001). Software Implementation of the NIST Elliptic Curves over Prime Fields. *D. Naccache, editor, Topics in Cryptology, CT-RSA 2001, volume LNCS 2020*. Berlin. Springer-Verlag: 250-265

Certicom Corporation. (1998). *The Elliptic Curve Cryptosystem for Smart Cards*. Certicom Research.

Certicom Corporation. (1999). *GEC2: Test Vector for SEC1*. Certicom Research.

Certicom Corporation. (2000a). *The Elliptic Curve Cryptosystem: Current Public-Key Cryptographic Systems.* Certicom Research.

Certicom Corporation. (2000b). *SEC2: Recommend Elliptic Curve Domain Parameters*. Certicom Research.

Certicom Corporation (2003). *The Next Generation of Cryptography*. Code and Cipher Vol. I, no. 1. Certicom Research.

Chong W. S. (2001). *Design of a Hash Processor Chip and The Implementation of a Digital Signature Subsystem for Data Security*. Universiti Teknologi Malaysia: M.Sc. Thesis.

Crowe F., Daly A., Kerins T., and Marnane W. (2004). *Single-Chip FPGA Implementation of a Cryptographic Co-processor*. Department of Electrical & Electronic Engineering, University College Cork. Unpublished.

Federal Information Processing Standards Publication (2001). *Advanced Encryption Standard*. U.S. FIPS PUB197.

Gupta V., Gupta S., Sheueling Chang. (2002). *Performance Analysis of Elliptic Curve Cryptography for SSL*. Sun Microsystems, Inc.

Institute of Electrical and Electronics Engineers (2000). *IEEE Standard Specification for Public-Key Cryptography*. New York, Std 1363-2000.

Ishii. S., Ohyama. K., Yamanaka K. (1994). A single-chip RSA processor implemented in a 0.5 μm rule gate array. *Proceedings, Seventh Annual IEEE Int. ASIC Conference and Exhibition*. September 19-23. IEEE: 433-436.

Johnson, D., Menezes, A. and Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1): 36-63.

Khalil. M. and Arul P. (2004). *Design of AES Processor*. Universiti Teknologi Malaysia. Ecad Research Laboratory Lab: Technical Report.

Khalil M. and Lim K. W. (2003). Design of an Elliptic Curve Cryptography (ECC) Processor Core for Implementation in FPGA-based System-on-Chip (SoC) Cryptosystem. *Proceedings of the 2003 Malaysian Science and Technology Congress (MSTC 2003)*. September 23-25. Kuala Lumpur, Malaysia.

Khalil. M. and Hau Y. W. (2004). Public Key Crypto Hardware for Real-Time Security Application. *Proceedings of the 2004 National Real-Time Technology and Applications Symposium (RENTAS 2004)*. November 14-15. Malaysia: UPM, 1-6.

Khalil. M, Hau Y. W and Arul Paniandi. (2005). An Implementation of Elliptic Curve Digital Signature Algorithm in FPGA-based Embedded System for Next Generation IT Security. *Proceedings of the 2005 International Conference on Robotics, Vision, Information and Signal Processing (ROVISP 2005)*. July 20-22. Malaysia: USM, 1-5.

Khalil. M, Arul Paniandi and Hau Y. W. (2005). RSA Crypto Processor for Resource-Constrained Mobile Embedded Systems. *Proceedings of the 2005 International Conference on Robotics, Vision, Information and Signal Processing (ROVISP 2005)*. July 20-22. Malaysia: USM, 130-135.

Kim H. W., Lee S. (2004). Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System. *IEEE Transactions on Consumer Electronics*. Vol. 50, No.1.

Kitsos P., Sklavos N., and Koufopavlou O. (2002). An Efficient Implementation of the Digital Signature Algorithm. Proc. 9th *IEEE International Conference on Electronics, Circuit and Systems.* September 2002. Vol III: 1151-1154.

Lejla Batina, Siddika Berna Ors, Bart Preneel, and Joos Vandewalle (2003). Hardware architectures for public key cryptography. *INTEGRATION the VLSI*: 1 – 64.

Li Y. C. (1998). *Hardware-Software Co-synthesis of Embedded Real Time Multiprocessors*. Princeton University: Ph.D. Dissertation.

Mathieu C., Michael N. Eric P. and JeanJacques Q. Parallel. (2003). FPGA Implementation of RSA with Residue Number Systems. *46th IEEE Midwest Symposium on Circuits and Systems*. Egypt.

Lim K. W. (2005). *An FPGA Implementation of an Elliptic Curve Processor for an Embedded Public-Key Cryptosystem.* Universiti Teknologi Malaysia: M.Sc. Thesis.

McIvor C., McLoone M. and McCanny J.V. (2004). Modified Montgomery Modular Multiplication and RSA Exponentiation Techniques. *Computers and Digital Techniques*. IEEE Proc. Volume 151, Issue 6:402-408.

McLoone M. and McCanny J.V. (2002). A Single-Chip IPSec Cryptographic Processor. *IEEE Workshop on Signal Processing Systems (SiPS) Design and Implementation*. California.

Menezes, A. J., van Oorschot, P. C. and Vanstone, S. A. (2001). *Handbook of Applied Cryptography*. Florida: CRC Press Inc.

National Institute of Standards and Technology (2001). *Introduction to Public Key Technology and the Federal PKI Infrastructure*. Computer Security Research Center.

National Institute of Standards and Technology (1995). *Secure Hash Standard.* FIPS PUB 180-1.

Nelson, M. (1996). *The Data Compression Book*. Hungry Minds.

Riedel I. (2003). *Security in Ad-hoc Networks: Protocols and Elliptic Curve Cryptography on an Embedded Platform*. Ruhr-University Bochum: Diploma Thesis.

Rissanen, J. (1983). A Universal Data Compression System. *IEEE Transaction. Information Theory*. IT-29: 656-664.

Rivest, R. L., Shamir, A. and Adleman, L. (1978). A Method for Obtaining Digital Signature and Public-Key Cryptosystems. *Communications of the ACM*. 21(2):120-126.

Rosing, M. (1999). *Implementing Elliptic Curve Cryptography*. Greenwich C.T.: Manning Publications.

RSA Data Security Inc. (1999). *Understanding Public Key Infrastructure (PKI).* RSA Data Security, Inc.

RSA Security Inc. (2000). *RSA Laboratories: Frequently Asked Questions about Today's Cryptography.* RSA Laboratories.

Saeki, M. (1997). *Elliptic Curve Cryptosystems.* McGill University: M.Sc. Thesis.

Stalling, W. (1999). *Cryptography and Network Security: Principles and Practice*. 2nd Ed. Upper Saddle River, New Jersey: Prentice Hall.

Steffen A. (2000) Secure Communications in Distributed Embedded Systems. *Security Group of the Zurich University of Applied Sciences*. Winterthur.

Sun Microsystems, Inc. (2001). *Public Key Infrastructure Overview*. Sun Microsystems, Inc.

Tan S. L. (2001). *An FPGA Implementation of RSA processor Core for Public Key Cryptosystem*. Universiti Teknologi Malaysia: M.Sc. Thesis.

Teh J-Wing. (2005). *Design of a Route Lookup Processor for Implementation in a FPGA-based System-on-Chip (SoC).* Universiti Teknologi Malaysia: M.Sc. Thesis.

Yeem K. M. (2002). *Design of a Data Compression Embedded Core for High-Speed Computing Applications.* Universiti Teknologi Malaysia: M.Sc. Thesis.